REMARKS

The Examiner is thanked for the thorough examination of the present application. The Office Action, however, has tentatively rejected all claims 1-16. Specifically, claims 1-16 stand rejected under 35 U.S.C 102(e) as allegedly anticipated by Kwan et al (U.S. 2004/0255154). Reconsideration of this application is respectfully requested in light of the remarks contained below.

Fundamental Distinction between Citations and the Present Invention

Applicant respectfully traverses the rejections of claims 1-16 of the present application for reasons that will be specifically addressed in following paragraphs. However, before addressing the details of specific rejections, Applicant notes that there are fundamental differences between the disclosure of the citation and that of the claimed embodiments.

The present application is generally directed to a method for detecting unauthorized hardware devices in a local area network, comprising scanning ports of a plurality of hardware devices to retrieve MAC addresses thereof, filtering an uplink port on each of the hardware devices to acquire a first MAC address list, calculating the number of MAC addresses of the filtered ports to acquire a second MAC address list, and subtracting the number of ports with more than two MAC addresses on the first MAC address list from the number of ports with more than two MAC addresses on the second MAC address list, thereby obtaining at least one unauthorized MAC address.

As described, embodiments of the invention detect multiple hardware devices, comprising network and computer devices, in a LAN and locates and excludes

unauthenticated network and computer devices from the hardware devices, enabling network stability and security.

In contrast, Kwan discloses a method for providing network security, comprising authenticating a physical address of a device coupled to a port of a network switch, and authenticating user information provided by a user of said device only if said physical address is valid. The Office Action alleged that the technical features of the claimed embodiments are disclosed in Kwan. Applicant respectfully disagrees.

With respect to disclosure of Kwan, there are multiple levels of security disclosed. The first level of security includes physical MAC address authentication of a device being attached to the network. A second level includes authentication of the user of the device. A third level includes dynamic assignment of the port to a particular VLAN based on the identity of the user, are applied. Failure to pass a lower security level results in a denial of access to subsequent levels of authentication.

In contrast, the claimed embodiments assign at least two MAC addresses to every port of a network device, one for the port of the centralized communication cable device and the other for the computer hardware device, uses relevant communication protocol (such as SNMP) to identify unauthorized network devices or computer hardware devices, and issues warning messages to users and to administrators to terminate the detection procedure.

Clearly, Kwan is quite different than the claimed embodiments, and for at least this fundamental reason, the rejections of all claims should be withdrawn.

Rejection of Claims 1, 7, and 12

Turning now to the specific rejections, referring to claim claims 1, 7, and 12, the claimed embodiments scan ports of a plurality of hardware devices to retrieve MAC addresses, filters an uplink port on each of the hardware devices to acquire a first MAC address list, calculates the number of MAC addresses of the filtered ports to acquire a second MAC address list, and performs a subtraction operation to obtains at least one unauthorized MAC address. Such a complete process and limitations are not disclosed in the citation.

As specifically embodied in the claims, independent claims 1, 7, and 12 specifically define:

> 1. A method for detecting unauthorized hardware devices in a local area network, comprising steps of:
>
> ***scanning ports of a plurality of hardware devices to retrieve MAC addresses thereof***;
>
> filtering an uplink port on each of the hardware devices to acquire a first MAC address list;
>
> ***calculating the number of MAC addresses of the filtered ports to acquire a second MAC address list;*** and
>
> subtracting the number of ports with more than two MAC addresses on the first MAC address list from the number of ports with more than two MAC addresses on the second MAC address list, thereby obtaining at least one unauthorized MAC address.
>
> 7. A system for detecting unauthorized hardware devices in a local area network, comprising:
>
> a device detection unit for ***scanning a plurality of ports of a plurality of hardware devices to retrieve MAC addresses thereof, filtering an uplink port of each hardware device to acquire a first MAC address list, and calculating the number of MAC addresses of the ports of the network devices to acquire a second MAC address list***; and
>
> a device processing unit, coupled with the device detection unit, for subtracting the number of ports with more than two MAC addresses on the first MAC address list from the number of ports with more than two MAC addresses on the second

MAC address list, thereby obtaining at least one unauthorized MAC address.

12. A storage medium containing a stored computer program providing a method for detecting unauthorized hardware devices, comprising using a computer to perform the steps of:

scanning a plurality of ports of a plurality of hardware devices to retrieve MAC addresses thereof;

filtering an uplink port of each hardware device to acquire a first MAC address list;

calculating the number of MAC addresses of the ports of the network devices to acquire a second MAC address list; and

subtracting the number of ports with more than two MAC addresses on the first MAC address list from the number of ports with more than two MAC addresses on the second MAC address list, thereby obtaining at least one unauthorized MAC address.

(*Emphasis added.*) Independent claims 1, 7, and 12 patently define over the cited art for at least the reason that Kwan fails to disclose at least the features emphasized above. This has been more particulary pointed out above in connection with the fundamental distinction.

As one example, the Office Action cited paragraphs [0009]-[0011], [0024], and [0036] of Kwan as allegedly teaching the claimed "scanning...." feature. In fact, these portions of Kwan actually state:

> [0009] In particular, the present invention is directed to a network device, such as a network switch, that implements a multiple key, multiple tiered system and method for controlling access to a data communications network in both a single host and multi-host environment. The system and method provide a first level of security that comprises authentication of the physical (MAC) address of a user device coupled to a port of the network device, such as a network switch, a second level of security that comprises authentication of a user of the user device if the first level of security is passed, such as authentication in accordance with the IEEE 802.1x standard, and a third level of security that comprises dynamic assignment of the port to a particular VLAN based on the identity of the user if the second level of security is passed.

[0010] The present invention provides improved network security as compared to conventional solutions, since it authenticates both the user device and the user. Moreover, the present invention provides network security in a manner more efficient than conventional solutions, since it performs physical (MAC) address authentication of a user device prior to performing the more resource-intensive step of performing user authentication, such as user authentication in accordance with a protocol defined by the IEEE 802.1x standard.

[0011] In accordance with one embodiment of the present invention, an apparatus for providing network security is provided. The apparatus includes a plurality of input ports and a switching fabric for routing data received on the plurality of input ports to at least one output port. The apparatus also includes control logic adapted to authenticate a physical address of a device coupled to one of the plurality of input ports and to authenticate user information provided by a user of the device only if the physical address is valid. Additionally, the control logic may be further adapted to assign the particular input port to a virtual local area network (VLAN) associated with the user information if the user information is valid. In an embodiment, the particular input port is assigned to the VLAN only if the apparatus is configured to support the specified VLAN.

[0024] The present invention is directed to a multiple key, multiple tiered network security system, method and apparatus. The system, method and apparatus provides at least three levels of security. The first level comprises physical MAC address authentication of a device being attached to a network, such as a device being coupled to a port of a network switch. The second level comprises authentication of the user of the device, such as authentication in accordance with the IEEE 802.1x standard. The third level comprises dynamic assignment of the port to a particular VLAN based on the identity of the user. Failure to pass a lower security level results in a denial of access to subsequent levels of authentication.

[0036] At step 304, network switch 102 performs a physical (MAC) address authentication of user device 108. As will be described in more detail herein, network switch 102 performs this step by comparing a MAC address of user device 108 with a limited number of "secure" MAC addresses that are stored by network switch 102. As shown at step 306, if packets received from user device 108 have a source MAC address that does not match any of the secure addresses, then the protocol proceeds to step 308, in which network switch 102 either drops the packets or, alternately, disables the port entirely, thereby terminating the security protocol. In a further embodiment of the present invention, network switch 102 can also re-direct the packets to a network destination other than their originally intended destination based on the detection of an invalid source MAC address.

As can be readily verified from even a cursory reading of the quoted portions of Kwan,

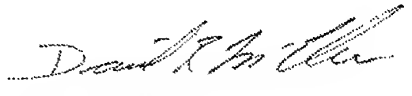
there is no teaching of the claimed "scanning a plurality of ports..." Thus, claims 1, 7, and 12 are novel based on the features of the Kwan citation and should be allowable.

Conclusion

As mentioned above, the embodiments of independent claims 1, 7, and 12 differ significantly from the cited art. Insofar as claims 2-6, depend from claim 1, claims 8-11, depend from claim 7, and claims 13-16, depend from claim 12, these claims are similarly believed to be patentable over the cited references

No fee is believed to be due in connection with this amendment and response. If, however, any fee is deemed to be payable, you are hereby authorized to charge any such fee to Deposit Account No. 20-0778.

Respectfully submitted,



Daniel R. McClure
Registration No. 38,962

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.
Suite 1750
100 Galleria Parkway N.W.
Atlanta, Georgia 30339
(770) 933-9500